UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/040,050	10/25/2001	Mahesh S. Maddury	50325-0598	1826

29989 7590 03/01/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
POWERS, WILLIAM S	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/040,050	MADDURY ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/14/2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Drawings

1. In light of Applicant's amendments, all previous objections to the drawings are withdrawn.

Claim Objections

2. In light of Applicant's amendments, all previous objections to claims 8-11 are withdrawn.

Claim Rejections - 35 USC § 112

3. In light of Applicant's amendments all previous rejections under 35 USC 112, 2nd paragraph are withdrawn.

Claim Rejections - 35 USC § 101

4. In light of Applicant's amendments, all previous rejections under 35 USC 101 are withdrawn.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 5, 6, 7, 10 and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent No. 5,414,772 to Naccache et al. (hereinafter Naccache).

As to claim 5, Naccache teaches determining a multiplicative inverse of a first integer value, y, through the processing means (column 4, lines 45-48) that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

As to claim 6, Naccache does not teach the use of the Extended Euclidean Algorithm (EEA) or the configuration of circuits to perform EEA operations (column 1, line 1-column 6, line 27).

As to claim 7, Naccache teaches that the multiplicative inverse is found through a series of steps (column 4, lines 35-61).

As to claims 10 and 11, Naccache teaches signing and verifying digital signatures (column 4, lines 58-61).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 1-4 and 12-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,414,772 to Naccache et al. (hereinafter Naccache) in view of Applicant admitted prior art.

As to claims 1,14 and 15, Naccache teaches:

a. Receiving and storing a first integer value, y, in memory means of a processing means of B (column 4, lines 40-44).

b. Determining that x is the multiplicative inverse of the first integer value, y, through the processing means (column 4, lines 45-48) that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

c. Storing x in a storage element for latter use in determining a digital signature (column 4, lines 45-61).

Naccache does not expressly mention that "the second quantity is two less than the prime modulus data value" in the modular exponentiation. However, in an analogous art, Euler's Theorem teaches that the exponent is two less than the prime modulus in a multiplicative inverse calculation (paragraph 43 of Specification).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the exponentiation means of Naccache with the exponent that is 2 less than the prime modulus in multiplicative inverse calculations of Euler. This is an accepted method for calculating the inverse with a prime modulus.

As to claims 2, 12 and 16 Naccache teaches:

a. Sending a first integer value, y, to an input of the processing means of B (column 4, lines 40-44), that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

b. Sending a second integer value, n, to an input of the processing means of B (column 3, lines 63-66), that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

c. Signing and verifying digital signatures (column 4, lines 58-61).

d. Decrypting and encrypting of messages (column 4, lines 58-61).

Naccache does not expressly mention sending a third value that is two less than the prime modulo. However, in an analogous art, Applicant uses Euler's Theorem that shows the exponent is two less than the prime modulus in a multiplicative inverse calculation (paragraph 43 of Specification).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the exponentiation means of Naccache with an exponent that is 2 less than the prime modulus in multiplicative inverse calculations of

Euler. This is an accepted method for calculating the inverse with a prime modulus as suggested by the Applicant.

As to claim 3, Naccache teaches:

a. Connections to send a first integer value, y, to an input of the processing means of B (column 4, lines 40-44), that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

b. Connections to send a other integer values to inputs of the processing means of B to determine the multiplicative inverse of the first integer, y (column 3, lines 63-66), that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

Naccache does not expressly mention connections for a third integer to be transmitted to a modular exponentiator as an exponent. . However, in an analogous art, Applicant uses Euler's Theorem that shows the exponent is two less than the prime modulus in a multiplicative inverse calculation (paragraph 43 of Specification).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the exponentiation means of Naccache with a connection to transmit an exponent that is 2 less than the prime modulus in multiplicative inverse calculations of Euler. This is an accepted method for calculating the inverse with a prime modulus as suggested by the Applicant.

As to claim 4, Naccache teaches:

a. Receiving a first integer value, y, to an input of the processing means of B (column 4, lines 40-44), that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

b. Receiving a second integer value, n, to an input of the processing means of B (column 3, lines 63-66), that include an exponentiation circuit, modular inversion circuit as well as other circuits (figure 2).

c. Outputting x, the multiplicative inverse of y, from apparatus B to apparatus A (column 4, lines 45-48).

Naccache does not expressly mention receiving a third value that is two less than the prime modulo. However, in an analogous art, Applicant uses Euler's Theorem that shows the exponent is two less than the prime modulus in a multiplicative inverse calculation (paragraph 43 of Specification).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the exponentiation means of Naccache with a connection to receive an exponent that is 2 less than the prime modulus in multiplicative inverse calculations of Euler. This is an accepted method for calculating the inverse with a prime modulus as suggested by the Applicant.

As to claim 13, Naccache teaches a processing means that include a circuit configured to perform exponentiation (column 3, lines 52-60).

11. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,414,772 to Naccache et al. (hereinafter Naccache) in view of US Patent No. 4,7594,063 to Chaum.

As to claims 8 and 9, Naccache does not expressly mention the use of the RSA encryption and decryption operations. However, in an analogous art, Chaum teaches the use of the RSA encryption and decryption operations with multiplicative inverses (column 4, line 58-column 5, line 29).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the exponentiation means of Naccache with the RSA encryption and decryption operations of Chaum (column 4, line 58-column 5, line 29) in order to protect message contents from being revealed to unauthorized third parties (column 3, lines 5-15) as suggested by Chaum.

Response to Arguments

12. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571 272 3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

William S. Powers
Examiner
Art Unit 2134

GUY LAMARRE
PRIMARY EXAMINER